Galois theory — Exercise sheet 1

https://www.maths.tcd.ie/~mascotn/teaching/2021/MAU34101/index.html

Version: September 24, 2021

Email your answers to mascotn@tcd.ie by Wednesday October 6, 4PM.

Exercise 1 *Fewer roots to generate the splitting field (100pts)*

1. Let K be a field such that $\operatorname{char} K \neq 2$, and let $F(x) = ax^2 + bx + c \in K[x]$ with $a \neq 0$. Finally, let $\overline{K}$ be an algebraic closure of K.

   Observe that $F(x) = a\left(\left(x + \frac{b}{2a}\right)^2 - \frac{\Delta}{(2a)^2}\right)$, where $\Delta = b^2 - 4ac$.

   (a) (10pts) Prove that there exists $\delta \in \overline{K}$ such that $\delta^2 = \Delta$.

   (b) (5pts) Express the roots of $F(x)$ in $\overline{K}$ in terms of δ.

   (c) (35pts) Suppose that Δ is not a square in K (in other words, that $\delta \notin K$). Prove that $F(x)$ is irreducible over K, and that $K(\delta)$ is both a stem field and a splitting field of $F(x)$ over K.

   (d) (15pts) Suppose now that $\delta \in K$. Describe a splitting field of $F(x)$ over K.

   (e) (5pts) What breaks down if $\operatorname{char} K = 2$? (The question merely asks you which part(s) of the logic go wrong; you are not required to find a way to fix what goes wrong.)

2. (30pts) Let K be a field, let $F(x) \in K[x]$ have degree $n \in \mathbb{N}$, and let $\alpha_1, \cdots, \alpha_n$ be the roots of $F(x)$ in an algebraic closure $\overline{K}$ of K, ordered in some arbitrary way. Prove that $K(\alpha_1, \cdots, \alpha_{n-1})$ is a splitting field of $F(x)$ over K.

   Hint: What is $\alpha_1 + \cdots + \alpha_n$*?*

This was the only mandatory exercise, that you must submit before the deadline. The following exercises are not mandatory; they are not worth any points, and you do not have to submit them. However, I highly recommend that you try to solve them for practice, and you are welcome to email me if you have questions about them. The solutions will be made available with the solution to the mandatory exercise.

Exercise 2 *Small non-prime finite fields*

1. Make a complete list of all finite fields (up to isomorphism) with at most 30 elements and which are not isomorphic to $\mathbb{Z}/p\mathbb{Z}$ for some prime $p \in \mathbb{N}$.
2. Give an explicit construction for each of them.
3. Make a list of all pairs (K, L) such that K and L are in your list and that L contains a copy of K (up to isomorphism).

Exercise 3 *Two models for* $\mathbb{F}_8$

Let $K = \mathbb{F}_2[x]/(x^3 + x + 1)$ and $L = \mathbb{F}_2[x]/(x^3 + x^2 + 1)$.

1. Prove that K and L are fields.
2. Prove that K and L are isomorphic.
3. Let $k(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$, so that $K = \mathbb{F}_2[x]/k(x)$. Establish a natural bijection between { isomorphisms from K to L } and { roots of $k(x)$ in L }.

   Hint: Prove that any morphism from K to L is automatically an $\mathbb{F}_2$-morphism. What does this imply about the image of the class of x in K by such a morphism?
4. Describe explicitly an isomorphism between K and L.

   Hint: Write $L = \mathbb{F}_2[y]/(y^3+y^2+1)$. Which equation does the class of $y+1 \in L$ satisfy? (Remember that $z = -z$ in characteristic 2, since $2z = 0$.)
5. Describe explicitly *all* the isomorphisms between K and L.

   Hint: Frobenius.

Exercise 4 *A formula for the discriminant*

Let $F(x) = x^n + bx + c \in \mathbb{C}[x]$, where $n \geqslant 2$ and $b, c \in \mathbb{C}$. Let $\beta \in \mathbb{C}$ be such that $\beta^{n-1} = -b/n$, and let $\zeta = e^{2\pi i/(n-1)}$, so that $\zeta^{n-1} = 1$ and that $x^{n-1} - y^{n-1} = \prod_{k=0}^{n-2}(x - \zeta^k y)$.

1. Express the roots of $F'(x)$ in terms of ζ and β.
2. Prove that $F(\zeta^k\beta) = \left(1 - \frac{1}{n}\right)\beta\zeta^k b + c$ for all $k \in \mathbb{Z}$.
3. Deduce that $\operatorname{disc} F = (-1)^{n(n-1)/2}\left((1-n)^{n-1}b^n + n^n c^{n-1}\right)$.
4. For which primes $p \in \mathbb{N}$ does the polynomial $x^5 - 5x + 6$ have multiple roots in $\overline{\mathbb{F}_p}$?